REMARKS

The Examiner rejected claims 1, 2, 4-10, 13, 22-24, 46 and 63-68 under U.S.C. §101 on the grounds that "the items 'configured to' perform various functionality could be embodied solely by software" (Final Action, page 4).

To expedite prosecution of the present application, Applicant amended independent claims 1, 22 and 46 to recite that the recited items comprise one or more programmable processing elements. Support for the amendments is provided throughout the present application, including, for example, at page 2, paragraphs 14-15, and at page 3, paragraph 39 of the published application (US 2004/0177145).

The Examiner rejected claims 1, 2, 4-10, 22-25, 46 and 56-71 under 35 U.S.C. §103(a) as being unpatentable over RFC 3325 Internet Draft (authored by Jennings and Peterson) in view of the reference "draft-ietf-sip-privacy-04.txt" by Marshall *et al.*, and further in view of "3GPP TSG SA WG3 Security - S3#18, Proposed changes to 33.2000 about Za, Zb, Zc interfaces" (hereinafter "3GPP"). The Examiner rejected claim 13 under 35 U.S.C. §103(a) as being unpatentable over Jennings in view of Marshall, and further in view of RFC 3574 by Soininen.

Applicant amended independent claim 1 to recite a feature that the forwarder is further configured to forward the message without modification in response to a determination (e.g., by the determiner) that the message has been through the security check applied at a security interface (e.g., a Za interface) prior to being received at the first network. Support for this amendment is provided throughout the present application, including, for example, at FIGS. 2a and 2b, and at page 4, paragraphs 53-59 of the published application. Applicant also amended independent claim 1 to clarify that the modifier modifies the message to include a second layer indication that the message has not been through the security check applied at the security interface prior to being received at the first network when the result of the determination is that the message has not been through the security check. Applicant similarly amended independent claims 22, 25 and 46. Additionally, Applicant cancelled claims 63, 66 and 69, and amended claims 64, 67 and 70 to correct their dependencies.

Applicant's independent claim 1 recites "a modifier, comprising the one or more programmable processing elements, configured to modify the message so as to include a second layer indication that the message has not been through the security check applied at a security interface between two security domains prior to being received at the first network when the result of the determination is that the message has not been through the security check, wherein the second layer is a higher layer than the first layer; wherein the forwarder is further configured to forward the message without modification in response to the determination being that the message has been through the security check applied at the security interface prior to being received at the first network." Thus, the message is modified by the modifier in response to a determination that the message has not been through a security check applied at a security interface (such as a Za interface), but is forwarded unmodified (e.g., by the forwarder) in response to the determination being that the message has been through a security check applied at the security interface:

> [0053] The first embodiment is represented by the steps in FIGS. 2a and 2b. Turning firstly to FIG. 2a, at the start of the process (30) a SIP message is received at the I-CSCF. This message could either have been received over the Za interface or directly from outside the network. In step 32, the I-CSCF 2 determines which of these two alternatives is the case.
>
> [0054] If the answer is no (i.e. message not received via Za interface), the I-CSCF 2 proceeds to step 34 at which a modification is made to the P-Asserted-Identity header of the message. In this embodiment a parameter is added to the header to indicate that the message has not been through security clearance. The example header shown above is therefore modified to have the following format:
>
> [0055] <sip:user1_public1@home1.net>;screening=no
>
> [0056] The I-CSCF then proceeds to step 36 in which the message, with the modified header is forwarded to the S-CSCF 6.
>
> [0057] If the answer to step 32 is yes, the message has come over the Za interface, and the I-CSCF proceeds directly to step 36 and forwards the message to the S-CSCF 6 without making any modifications to the message.
>
> [0058] At step 38 the message arrives at the S-CSCF bearing an indication of its authenticity. In other words, if the message arrives

> with a normal P-Asserted-Identity header, the S-CSCF 6 knows that it has been through a security check.
>
> [0059] If the message arrives with a modified P-Asserted-Identity header, the S-CSCF 6 knows that it has not been through a security check.
>
> (US 2004/0177145, FIGS. 2a and 2b, and page 4, paragraphs 53-59)

In rejecting claim 1, the Examiner admitted that "Jennings does not, however, explicitly show all of: determining whether or not a message has been received with security at a first layer; a modifier configured to modify the message so as to indicate a second layer indication that the message has not been though a security check at the first layer prior to being received at the first network when the result of the determination is that the message has not been through a security check, wherein the second layer is a higher layer than the first layer" (Final Action, pages 5-6).

It follows, therefore, that Jennings also fails to disclose "a modifier, comprising the one or more programmable processing elements, configured to modify the message so as to include a second layer indication that the message has not been through the security check applied at a security interface between two security domains prior to being received at the first network when the result of the determination is that the message has not been through the security check, wherein the second layer is a higher layer than the first layer," as recited in independent claim 1.

Additionally, inasmuch that Jennings does not show "determining whether or not a message has been received with security at a first layer" (as admitted by the Examiner at page 5 of the Final Action), Jennings also does not describe that the message is forwarded unmodified in response to determining that the message has been through the security check applied at the security interface. Thus, it follows that Jennings also does not disclose or suggest at least the features of "wherein the forwarder is further configured to forward the message without modification in response to the determination being that the message has been through the security check applied at the security interface prior to being received at the first network," as recited in independent claim 1.

Marshall described "extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems, and to convey indications of end-user requested privacy" (Marshall, Abstract). Marshall explains that when a message from an untrusted entity is received by a proxy, the proxy examines if the message includes Remote-Party-ID header so that the proxy can verify the Remote-Party-ID header. If the verification is successful, the proxy adds an "rpi-screen" parameter that is set to "yes", and if the verification fails, the proxy adds an "rpi-screen" parameter that is set to "no". On the other hand, if the message was received from a trusted entity, the proxy does not apply any special processing to the message and simply forwards the message to the next hop.

> 7.5 Proxy Behavior
>
> When a proxy supporting this extension receives an INVITE, OPTIONS, REGISTER or extension method request from a trusted entity, it does not apply any special processing until the message is forwarded to the next hop. If the message instead came from an untrusted entity, the proxy MUST do the following:
>
> First, the proxy MUST examine the message for the presence of any Remote-Party-ID headers. Since the request was received from an untrusted entity, each of these MUST either be verified by the proxy or have their rpi-screen parameter set to "no". If the proxy is able to successfully verify the information in a Remote-Party-ID header field (by means outside the scope of this document), the proxy MUST add an rpi-screen parameter set to "yes" for that Remote-Party-ID. Furthermore, this MUST be the only rpi-screen parameter for that Remote-Party-ID. If verification fails however, further processing depends on the reason for the failure. Two different failure reasons are defined here:
>
> * The information provided could not be verified because the proxy does not support verification of the identity information for this particular Remote-Party-ID.
> * The proxy supports verification of this particular Remote-Party-ID, however the identity information provided is incorrect and the proxy detected that, or the identity information could not be verified.
>
> In the first case, the proxy MUST add an rpi-screen parameter set to "no". The proxy SHOULD furthermore ensure this is the only rpi-screen parameter. In the second case, the proxy MUST by default add an rpi-screen parameter set to "no" and ensure this is the only rpi-screen parameter, however individual extensions and local

> procedures MAY specify a different behavior, for example rewrite or removal of the offending Remote-Party-ID header field.
>
> (Marshall, Section 7.5)

Thus, Marshall's proxy adds an "rpi-screen" parameter when the message was received from an untrusted entity. However, even assuming, for argument's sake, that receiving a message from an untrusted entity implies that a security check has not been performed prior to the message having been received at the proxy, Marshall in any event does not describe that the addition of an "rpi-screen" parameter is performed in response to performing a security check applied at a security interface between two security domains. Indeed, Marshall does mention applying a security check at a security interface. Furthermore, as noted, receiving a message from an untrusted entity does not imply that no security has been performed.

Accordingly, Marshall fails to disclose or suggest at least the features of "a modifier, comprising the one or more programmable processing elements, configured to modify the message so as to include a second layer indication that the message has not been through the security check applied at a security interface between two security domains prior to being received at the first network when the result of the determination is that the message has not been through the security check, wherein the second layer is a higher layer than the first layer," as recited in claim 1.

Additionally, while Marshall also describes forwarding the message without processing it if the message was received from a trusted entity, at no point does Marshall describe that the message is forwarded without processing if it is determined that a security check was applied to the message at a security interface between two security domains. Indeed, a determination that a message was received from a trusted entity is not the same as determining that a security check at a security interface between two security domains was applied to the message.

Accordingly, Marshall also fails to disclose or suggest at least the features of "wherein the forwarder is further configured to forward the message without modification in response to the determination being that the message has been through the security check applied at the security interface prior to being received at the first network," as recited in claim 1.

3GPP, which describes security interfaces, such as Za and Zb interfaces, does not describe performing certain operations (e.g., modifying a message or forwarding a message unmodified) based on a determination of whether a security check was applied to a message to any of the interfaces described by 3GPP. Thus, 3GPP fails to cure the deficiencies of the teachings of Marshall and/or Jennings as they relate to the features discussed above. Accordingly, 3GPP too fails to disclose or suggest at least the features of "a modifier, comprising the one or more programmable processing elements, configured to modify the message so as to include a second layer indication that the message has not been through the security check applied at a security interface between two security domains prior to being received at the first network when the result of the determination is that the message has not been through the security check, wherein the second layer is a higher layer than the first layer," and/or "wherein the forwarder is further configured to forward the message without modification in response to the determination being that the message has been through the security check applied at the security interface prior to being received at the first network," as recited in independent claim 1.

Because none of the references discloses or suggests, alone or in combination, at least the features of "a modifier, comprising the one or more programmable processing elements, configured to modify the message so as to include a second layer indication that the message has not been through the security check applied at a security interface between two security domains prior to being received at the first network when the result of the determination is that the message has not been through the security check, wherein the second layer is a higher layer than the first layer," and/or "wherein the forwarder is further configured to forward the message without modification in response to the determination being that the message has been through the security check applied at the security interface prior to being received at the first network," Applicant's independent claim 1, and the claims depending from it, are patentable over the cited art.

Applicant's independent claims 22, 25 and 46 recite "a network processing element, comprising the one or more programmable processing elements, the security server being configured to receive a message, determine whether the message has

been through a security check by determining whether or not the message has been received with security at a first layer, when the result of the determination is that the message has not been through the security check applied at a security interface between two security domains modify the message so as to include a second layer indication that the message has not been through the security check applied at the security interface prior to being received at the security server, wherein the second layer is a higher layer than the first layer, and forward the message regardless of the result of the determination; wherein the network processing element is configured to forward the message without modification in response to the determination being that the message has been through the security check applied at the security interface prior to being received at the first network," or similar language. For reasons similar to those provided with respect to independent claim 1, independent claims 22, 25 and 46, and the respective claims depending from them, are patentable over the cited art.

CONCLUSION

On the basis of the foregoing amendments, the pending claims are in condition for allowance. It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper. Applicant asks that all claims be allowed.

If there are any questions regarding these amendments and remarks, the Examiner is encouraged to contact the undersigned at the telephone number provided below. The Commissioner is hereby authorized to charge any additional fees that may be due, or credit any overpayment of same, to Deposit Account No. 50-0311, reference No. 39700-591001US.

Respectfully submitted,

Date: May 7, 2010

Ido Rabinovitch
Reg. No. L0080

Address all written correspondence to
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.
One Financial Center
Boston, Massachusetts 02111
Customer No. 64046
Telephone: 617-348-1806
Facsimile: 617-542-2241